Нефункциональные требования к ERP

Кумтор Голд Компани

# Содержание

[Содержание 2](#_Toc92192270)

[1. Архитектура системы 4](#_Toc92192271)

[1.1. Общие требования к системе 4](#_Toc92192272)

[1.2. Требования к языкам программирования 4](#_Toc92192273)

[1.3. Требования к протоколам обмена данными при интеграции информационных систем 4](#_Toc92192274)

[1.3. Расположение данных 5](#_Toc92192275)

[1.4. Пользовательский интерфейс 5](#_Toc92192276)

[1.4. Модуль администрирования пользователей 6](#_Toc92192277)

[1.5. Отчетность 6](#_Toc92192278)

[1.6. Процесс изменения в ПО 6](#_Toc92192279)

[2. Производительность 6](#_Toc92192280)

[2.1. Мониторинг производительности 7](#_Toc92192281)

[2.2. Сбалансирование нагрузки 7](#_Toc92192282)

[2.3. Информация о пользователей системы 7](#_Toc92192283)

[3. Документация 8](#_Toc92192284)

[3.1. Обучение 8](#_Toc92192285)

[4. Информационная Безопасность 8](#_Toc92192286)

[4.1. Персональные данные 9](#_Toc92192287)

[4.2. Коммерческая тайна 10](#_Toc92192288)

[4.3. Защита машинных носителей информации 10](#_Toc92192289)

[4.4. Авторизация и аутентификация 10](#_Toc92192290)

[4.5. Данные 10](#_Toc92192291)

[4.6. Физические требования 11](#_Toc92192292)

[4.7. Киберугрозы 11](#_Toc92192293)

[4.8. Ограничение программной среды 11](#_Toc92192294)

[4.9. Защита среды виртуализации 11](#_Toc92192295)

[5. Классификация ERP системы по приоритету восстановления 12](#_Toc92192296)

[5.1. Классификатор ERP системы по типу обработки отказов 12](#_Toc92192297)

[5.2. Классификатор ERP системы по времени восстановления и доступности за год 14](#_Toc92192298)

[5.3. Классификатор ERP системы по звенности 15](#_Toc92192299)

[5.4. Классификатор ERP системы по избыточности 15](#_Toc92192300)

[5.5. Классификатор ERP системы по режиму поддержки 15](#_Toc92192301)

[5.6. Классификатор ERP системы по способу обработки отказов 15](#_Toc92192302)

[5.7. Классификатор ERP системы по этапам (статусам) жизненного цикла платформы и архитектуры 15](#_Toc92192303)

[5.8. Классификатор ERP системы по производителям оборудования и системного ПО 16](#_Toc92192304)

[5.9. Классификатор ERP системы по уровню мониторинга 16](#_Toc92192305)

[5.10. Классификатор ERP системы по категориям пользователей 16](#_Toc92192306)

[5.11. Классификатор ERP системы по типу масштабирования 16](#_Toc92192307)

[5.12. Типовой архитектурный шаблон для ERP системы 16](#_Toc92192308)

# 1. Архитектура системы

ERP система должна иметь 3-звенную архитектуру приложения, т.е. должна состоять из клиентской части, сервера приложения и СУБД.

## 1.1. Общие требования к системе

* Система должна быть модульной. Определенный набор функционала должен быть реализован в модуле системы, т.е. не должно быть функционала реализованного в одном ядре без расширяющих модулей (конкурентным преимуществом будет использование микросервисной архитектуры);
* Система должна позволять развертывание в облачных дата центрах (Microsoft Azure, AWS, Google и др.). Конкурентным преимуществом будет если приложение cloud – native с API функционала системы, с поддержкой контейнеризации (dockers) и использованием Open Shift оркестратора;
* Система должна позволять масштабироваться (вертикально и горизонтально). Конкурентным преимуществом будет считаться наличие горизонтального масштабирования;
* Система должна использовать промышленные стандарты и технологии;
* Система должна иметь встроенные инструменты мониторинга работоспособности системы (API для отслеживания состояния системы, оценка работоспособности и качества бизнес – процессов, средства конфигурирования и оперативного управления)
* Наличие возможности анализа и моделирования бизнес - процессов (what if, GAP analysis, scenario analysis), алгоритмы прогнозирования сценарных анализов и стратегий c использованием алгоритмов машинного обучения (Machine Learning);
* Система должна быть кроссплатформенной (работать с операционными системами Oracle Linux, Centos, Windows);
* Система должна иметь встроенные средства CI / CD (Continuous Integration / Continuous Deployment), систему контроля версий прикладного программного обеспечения, либо использовать Open Source (конкурентным преимуществом будет предоставление бесплатно встроенных средств CI / CD, либо настроенных под систему Open Source инструментов для CI / CD).

## 1.2. Требования к языкам программирования

ERP система должна поддерживать следующие языки программирования:

* Java EE
* Java Script
* ASP.NET
* C#
* ABAP

## 1.3. Требования к протоколам обмена данными при интеграции информационных систем

ERP система должна поддерживать информационный обмен данными посредством API (использование микросервисов на Java SpringBoot будет являться конкурентным преимуществом).

Интеграционная технология системы должна поддерживать один из следующих протоколов передачи данных: JSON (RPC), gRPC, XML (RPC), HTTPS,batch import

В качестве технологии и стандартов обмена данными будет приветствоваться преимущественными поддержка технологий RESTful API и SOAP.

## 1.3. Расположение данных

Решение ERP системы (SaaS) / On Premise должно быть развернуто в Центрах Обработки данных в Кыргызской Республике. Вендор / Поставщик ERP должен самостоятельно найти Партнера (владельца Центра Обработки данных) на территории Кыргызской Республики для основного центра обработки данных в соответствии с требованиями к ERP системе пункта 5. “Классификация ERP системы по приоритету восстановления”.

Резервный центр обработки данных будет находиться в серверной Рудника КГК.

Конкурентным преимуществом будет решение ERP системы с использованием SaaS.

## 1.4. Пользовательский интерфейс

Система должна иметь пользовательский интерфейс на тонком клиенте / веб браузер, адаптивный дизайн веб интерфейса под смартфоны и планшеты. Наличие мобильных приложений на iOS, Android будет являться конкурентным преимуществом.

Клиентское приложение должна быть доступна через веб и мобильные приложения по протоколу HTTPS.

Система должна иметь опцию выбора языка, на котором необходимо отображать Юзер интерфейс для конечного пользователя. Английский и Русский языки обязательно должны присутствовать для выбора. Кроме этого, система должна поддерживать региональные установки Россия, Кыргызстан для обработки дат и чисел.

Пользовательский интерфейс должен иметь возможность отображать самих данных системы в юникоде, т.е. независимо от языка данных.

По технологию хранения и обработки данных клиентское ПО должно иметь возможность локального кеширования и обработки данных. При возникновения сбоя на стороне сервера или недоступности сервера, клиентское приложение должно иметь возможность локально завершить обработку данных текущей функции и хранить данные до полного возобновления работоспособности системы.

Пользовательский интерфейс должен быть дружелюбным и удобным для пользователей. Программа должна иметь подсказки и указателей на функциональные компоненты приложения. Приложения предназначенные на обработку больших данных должны иметь функции автоматической обработки данных, например такие как копирование, дублирование, импорт/экспорт из Excel файла, авто размножение, ввод и утверждение одинаковых данных на множество линий и т.д. При возникновении ошибки или сбоя, ПО должно выдавать соответствующее информационное сообщение/уведомление, понятное конечному пользователю.

Должна быть функция авто сохранения при вводе несколько этапных и больших данных в процессе работы незавершенной функции. У пользователя должна быть возможность продолжить процесс с того места, которое было сохранено в последний раз.

В главной странице клиентского ПО должны быть доступны ссылки/команды перехода на последние или самые активные за последнее время приложения. Должен быть отображен список документов или транзакций в виде гиперссылки, требующих внимания пользователя, при нажатии которых пользователь должен попасть на необходимое приложение для обработки.

## 1.4. Модуль администрирования пользователей

Система должна включать в себя модуль администрирования пользователей, т.е. список ролей, прав доступа к объектам данных и записям данных (CRUD – Create, Read, Update, Delete).

## 1.5. Отчетность

Стандартные отчеты ERP должны быть доступны конечным пользователям в главном окне ПО согласно ролю и матрице доступа. Возможность настройки полей, параметров и формата отображения отчетов на стороне клиента приветствуется как преимущественная опция.

Должна быть опция для выгрузка отчета в Excel, PDF без ограничения по количеству строк в отчете. Отправка отчета по электронной почте должна быть автоматизирована внутри приложения.

Должна быть доступна аналитическая отчетность по данным всех модулей системы. Аналитическая платформа должна быть настраиваемая по обновлению данных. Мониторинг и контроль за ETL процессом для аналитической системой отчетности должна быть на стороне клиента. Высокая производительность по отображению больших данных приветствуется.

## 1.6. Процесс изменения в ПО

Любое изменение в ПО должно проходить всю процедуру по изменению/разработки (SDLC) согласно требованиям аудита и политикам ИТ КГК начиная от заявки до деплоймента. Т.е. должен быть соблюден весь процесс по изменению (Change), утвержденный в ИТ КГК.

Система должна иметь наличие минимум 4-х сред(платформ) по поддержке разработок и изменений:

1. Разработческая (Development platform)
2. Тестовая платформа (Test platform)
3. Пред промышленная платформа (Preproduction platform) – максимально приближенная к рабочей версии.
4. Рабочая промышленная платформа (Production platform)

# 2. Производительность

Система должна быть способной обрабатывать функции и запросы от 1,000 пользователей, подключенных и работающих в системе одновременно.

Время отклика серверного приложения на средний запрос клиентского приложения не должно быть более 0.5 с. Транзакционная обработка при сохранении данных должна быть независимой от процесса блокировки таблиц данных по приоритетам. Одновременное редактирование одних и тех же данных разными пользователями не должно допускаться.

Клиентское приложение должно передавать данные к серверу по каждой микрооперации во избежание обработки больших данных. Тайм аут обработки запроса не должен превышать 30 секунд.

## 2.1. Мониторинг производительности

На стороне сервера должна быть установлена мониторинговая система по производительности (например Zabbix), которая следит за производительностью обработки данных сервисов системы и по заданному интервалу времени рассылает отчет о производительности системы за указанный период. При необходимости пользователь должен иметь возможность запросить отчет о производительности за любой период.

## 2.2. Сбалансирование нагрузки

Система должна иметь балансирующую технологию по разгрузке обработки данных на стороне сервера. Например как наличие балансирующих онлайн сервисов по обработке запросов клиентских приложений и автоматическое переключение между ними при необходимости перезагрузки. Серверное приложение по обработке данных должна функционироваться независимо от процесса системы управления базой данных (СУБД).

## 2.3. Информация о пользователей системы



# 3. Документация

По проекту исполнитель должен предоставить/приготовить и согласовать с заказчиком следующие документы:

* Коммерческое предложение;
* Организационная структура проекта, с указанием ролей, ответственностью со стороны Вендора / Поставщика, КГК;
* Устав Проекта, План управления Проектом;
* План проекта с указанием ресурсов и ролей в проекте, со стороны Вендора / Поставщика, КГК, задачами и их артефактами, вехами, датами по задачам и фазам
* Техническое задание на внедрение информационной системы (с описанием сервисов по интеграции с др. системами);
* Архитектура решения (логическая структура приложения, с разбивкой на модули; функциональная архитектура; сценарии интеграции приложений; схема развертывания системы в отказоустойчивой архитектуре, в разбивке сред – разработка, тест, препрод, прод);
* Сайзинг на аппаратное обеспечение системы, в разбивке сред (разработка, тест, препрод, прод);
* Программа и методика испытаний c тест - кейсами, результаты тестирования;
* Соглашение об уровне обслуживания (SLA), в соответствии с требованиями КГК (стандарты классов ИТ систем);
* Руководство пользователя, онлайн help (User manual)
* Руководство администратора (Administrator manual)
* Руководство администратора безопасности (Security Administrator manual)
* Руководство программиста (Programmer guide)
* Руководство системного администратора
* Руководство администратора баз данных
* Описание процедуры по изменениям (SDLC process description)

## 3.1. Обучение

Исполнитель должен провести обучение всех пользователей системы (Администраторы приложений, системные администраторы, администраторы баз данных, разработчики, группа техподдержки 1-й и 2-й линии, простые пользователи). Все простые пользователи должны пройти обучение по использованию ПО каждый по своей области бизнес процессов и по общим функциям.

Требуется отдельная автоматизированная система или методология по обучению пользователей к ERP системе для дальнейшей поддержки знания у пользователей КГК.

# 4. Информационная Безопасность

Система должна иметь функцию авто логирования и журналирования всех изменений / событий на стороне сервера. Необходимо иметь настройку по логированию изменений по направлениям:

* Административные изменения
* Пользовательские изменения
* Системные изменения

На стороне клиентского приложения должна быть доступна функция логирования всех шагов при необходимости. Такая функция должна хранить следующих данных как минимум: Идентификатор пользователя, время, имя запущенной функции, имя команды, входные/выходные параметры, возможные ошибки и т.д.

Система должна иметь админ приложение для управления и администрирования доступов, ролей и групп пользователей в разрезе функций, приложений и модулей ПО. Модули и приложения системы должны быть доступны конечным пользователям согласно матрице доступа (CRUD). Кроме этого, наличие консоль приложения на стороне сервера для управления супер конфиденциальными настройками и доступами, будет иметь преимущество.

Передаваемые данные между сервером и клиентом, а также между сервер приложением и СУБД, должны быть зашифрованы. Алгоритм и ключ шифрования должна быть максимально секретным и иметь длину ключа не менее 1024 Бит.

Аутентификация пользователей в системе должна иметь возможность подключения к актив директории (AD) компании и выполнить аутентификацию по SSO с применением MFA.

Авторизация пользователей должна быть в модуле администрирования пользователей и прав доступа.

Аутентификация и авторизация пользователей должна быть многофакторной, точнее должна быть двухфакторной.

Необходимо наличие функции автоблокировки клиентской сессии/приложения при истечении определенного времени бездействия конечного пользователя. Среднее время для автоблокировки от 10 минут до 1 часа, оно должно быть настраиваемое согласно требованиям и политикам информационной безопасности КГК.

Для всех разработчиков и пользователей системы доступ к СУБД должен быть в режиме только чтения (Read only). Для администраторов ERP системы доступ на изменения в СУБД должен быть предоставлен только во время имплементации и только по утверждению заявки по изменению (Change) высшим руководством ИТ КГК.

## 4.1. Персональные данные

Все данные системы, которые относятся к категориям персональных данных работников КГК, должны физически храниться и обрабатываться только на территории КР согласно закону о персональных данных КР. К таким категориям данных относятся данные, обрабатываемые в системах управления персоналом (HR) и расчета заработных плат работников (Payroll).

## 4.2. Коммерческая тайна

Все данные системы, которые относятся к категориям информации и данным коммерческого характера в системе, должны храниться и обрабатываться согласно закону КР о коммерческой тайне.

## 4.3. Защита машинных носителей информации

Для защиты машинных носителей информации должны выполняться следующие требования:

* Учет машинных носителей информации.
* Управление доступом к машинным носителям информации.
* Контроль перемещения машинных носителей информации за пределы контролируемой зоны.
* Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.
* Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации.
* Контроль ввода (вывода) информации на машинные носители информации. Контроль подключения машинных носителей информации.

Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания).4.4 Требования информационной безопасности к SAAS

## 4.4. Авторизация и аутентификация

Система должна предоставлять защиту и управление доступом для функций, основанных на полномочиях. Система должна предоставлять механизм, позволяющий администратору создавать, изменять и удалять учетные записи пользователей в выделенном собственном каталоге пользовательских учетных записей. Пользовательские данные могут размещаться в информационной среде внутри предприятия. Система должна предоставлять механизмы аутентификации пользователей с использованием данных, размещенных во внутренней информационной среде, и авторизации с использованием данных управления доступом, предоставляемых по требованию.

## 4.5. Данные

Изоляция данных и исполнение нормативных требований пользовательских данных для размещения в выделенной базе данных. Система должна предоставлять механизм аутентификации и авторизации пользователей в изолированной области базы данных, настроенной специально по требованиям, которые принадлежат пользователям. База данных клиента должна быть изолирована от баз данных других клиентов. Обработка данных клиента должна происходить в выделенном сегменте, изолированном от других систем провайдера. Данные должны храниться только в зашифрованном виде. Передача данных должна происходить только по защищенным каналам и протоколам. Доступ в базу данных должен предоставляться авторизированным и аутентифицированным пользователям.

## 4.6. Физические требования

Инфраструктура провайдера должна позволять переносить мощности на резервное оборудование в случае недоступности основного в течение сроков по SLA. Основное и резервное оборудование провайдера должно быть разнесено по территориальному признаку.

## 4.7. Киберугрозы

Сервисы безопасности провайдера должны обеспечивать предотвращение вторжений (IDS / IPS). Провайдер должен обеспечить защиту от специфических облачных угроз. Провайдер должен обеспечивать защиту информации от вирусов, зловредного кода и уязвимости 0-го дня. Провайдер должен обеспечить защиту своих мощностей от стандартных угроз таких, как утечка информации, сетевые атаки типа “отказ в обслуживании” (DoS/DDoS) и прочих уязвимостей, приводящих к простою сервиса.

## 4.8. Ограничение программной среды

Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения. Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов. Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов.

## 4.9. Защита среды виртуализации

Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин. Регистрация событий безопасности в виртуальной инфраструктуре. Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры. Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных. Контроль целостности виртуальной инфраструктуры и ее конфигураций. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры. Реализация и управление антивирусной защитой в виртуальной инфраструктуре. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

4.5 Требования информационной безопасности к решению On Premise согласно проектной документации на стадии предпроектного решения!

# 5. Классификация ERP системы по приоритету восстановления

Согласно стандартам и классам ИТ КГК, система ERP по приоритету восстановления входит в класс ИТ систем **BC “Business Critical”**. Бизнес критичные системы – это системы, недоступность которых оказывает немедленное негативное влияние на способность компании получать доходы, или оказывает критическое влияние на эффективность работы большого количества сотрудников компании КГК. Иными словами, это системы, обеспечивающие поддержку бизнес деятельности компании КГК.

|  |  |  |
| --- | --- | --- |
| **Код класса Системы** | **Имя класса Системы** | **Описание классификаторов** |
| BC | Business Critical | Недоступность этих Систем в течение 1 суток приводит к значительным косвенным производственным потерям, в результате которого компания КГК понесет существенные экономические потери в бизнесе. |

В ERP систему входят след бизнес процессы КГК:

* Управление финансами
* Управление техобслуживания и ремонтов
* Управление активами компании
* Управление закупками и цепью поставок
* Управление логистикой (перевозками)
* Управление рисками и комплаенс (Governance, Risk and Control);
* Управление складом

***Опционально:***

* Управление партнерами

Более подробно изложена в функциональном требовании.

## 5.1. Классификатор ERP системы по типу обработки отказов

По типу обработки отказов, ERP система подпадает в класс **FT “Fault Tolerance”**. По уровню критичности и значимости модулей, ERP система должна быть обеспечена механизмом восстановления в самом основном ЦОДе автоматически и в резервном ЦОДе вручную при необходимости.

|  |  |  |
| --- | --- | --- |
| **Код классифи****катора** | **Имя классификатора** | **Описание** |
| FT | Fault Tolerance | Обеспечивает полное дублирование оборудования в пределах основного ЦОДа и автоматическое\полуавтоматическое восстановление работоспособности IT-Системы (автоматическое\полуавтоматическое переключение на резервное оборудование), или полное дублирование оборудования в резервной ЦОДе и ручное восстановления работоспособности ИТ-Системы (Ручное переключение на резервное оборудование) |

## 5.2. Классификатор ERP системы по времени восстановления и доступности за год

По требованиям восстановления и доступности ERP система подпадает на классификатор RC3 “**High Speed+**”. Ниже в таблице показаны требования к данному классу согласно стандартам ИТ КГК.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код шаблона отказоус тойчивос ти | Имя шаблона отказоус тойчивос ти | Описание шаблона | Код класса Системы использую щий данный шаблон | Регламентир ованный % доступности Системы за год (SLA) | Макс. допустимое время простоя Системы за год | \*Восстановление в случае локального сбоясистемы | \*Восстановление в случае падения основного ЦОДа | Количество необходимых комплектов оборудования для обеспечения заявленной отказоустойчивости |
| RC3 | HighSpeed | Системы, недоступность которых влияет на невозможность получения доходов в долгосрочной перспективе, или существенно влияет на эффективность работы большого количества сотрудников компании КГК. Т.е. это системы, обеспечивающие поддержку различных операций компании КГК. Недоступность этих Систем в течение 1 суток не приводит к существенным финансовым потерям. | BC | 99,6% | До 1д 11ч 3м | до 60 мин | 0-30 мин | До 60 мин | 0-30 мин | Один комплект в основном ЦОДе и один комплект в резервном ЦОДе (всего 2 комплекта оборудования) |

## 5.3. Классификатор ERP системы по звенности

По типам звенности ERP система должна состоять как минимум из двух звенной или трехзвенной системы.

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| 3U | Трехзвенная | Компоненты (Front, Middle, DB) IT-Системы распределены нааппаратных либо виртуальных серверах, либо совмещённый вариант. |

## 5.4. Классификатор ERP системы по избыточности

Система должна иметь возможность балансировки нагрузки по избыточности между серверами

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| FRB | Полностью резервированная сбалансировкой нагрузки | Все компоненты IT-Системы имеют резервное оборудование с возможностью балансировки нагрузкимежду основным и резервным оборудованием. |

## 5.5. Классификатор ERP системы по режиму поддержки

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| S24x7 | S24x7 | IT-Система, сопровождаемая IT в режиме 24 часа в сутки и 7дней в неделю. |

## 5.6. Классификатор ERP системы по способу обработки отказов

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| MAR | Полуавтоматическоевосстановление | Восстановление IT-Системы требует вмешательства дежурнойсмены инженеров и наличие инструкций по восстановлению. |

## 5.7. Классификатор ERP системы по этапам (статусам) жизненного цикла платформы и архитектуры

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| PER | Перспективная | IT-Система, архитектура и платформа которой удовлетворяеттекущим IT Стандартам компании и учитывает тенденции развития ИТ-индустрии на долгосрочную перспективу. |

## 5.8. Классификатор ERP системы по производителям оборудования и системного ПО

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| FC | Сертифицированная IT | IT-Система, все компоненты которой предполагаютиспользование стандартного для IT компании оборудования и системного ПО. |

## 5.9. Классификатор ERP системы по уровню мониторинга

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| FM | Доступна для пользователей | IT-Система является объектом комплексного автоматического мониторинга, способного с минимальной задержкой определить недоступность системы для конечного пользователя и предпринять корректирующиевоздействия. |

## 5.10. Классификатор ERP системы по категориям пользователей

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| AB+ EC | Внешние и внутрениипользователи | IT-Система, пользователями которой являются как ивнешние так и внутрение пользователи. |

## 5.11. Классификатор ERP системы по типу масштабирования

|  |  |  |
| --- | --- | --- |
| **Код** | **Имя** | **Описание** |
| VM/GM | Гибридноемасштабирование | IT-Система позволяет производить масштабирование как в“вертикальном” так и “горизонтальном” направлении. |

## 5.12. Типовой архитектурный шаблон для ERP системы

Для ERP системы подходит типовой шаблон “High Speed+RC3”.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Код шаблона отказоус тойчивос ти** | **Имя шаблона отказоуст ойчивост и** | **Описание шаблона** | **Восстановление в случае локального сбоя системы** | **Восстановление в случае падения основного****ЦОДа** |
| **RTO** | **RPO** | **RTO** | **RPO** |
| RC3 | High Speed | Системы, недоступность которых влияет на невозможность получения доходов в долгосрочной перспективе, или существенно влияет на эффективность работы большого количества сотрудников компании КГК. Т.е. это системы, обеспечивающие поддержку различных операций компании КГК. Недоступность этих Систем в течение 1 суток не приводит к существенным финансовым потерям. | 60 мин | 0-30 мин | 60 мин | 0-30 мин |

Системы класса RC3 по приоритету восстановления - это Системы **BC (Business Critical)**, а по типу обработки отказов – **FT (Fault Tolerance)**.

Могут применять следующие технологии резервирования данных:

1. РКД по сети LAN или SAN;
2. РКД данных на дисковую память;
3. РКД на магнитные ленты.

Схема восстановления Систем класса RC3 (High Speed)



Резервный ЦОД – это серверная Рудника.

**Для класса RC3 должны быть учтены следующие требования:**

1) необходимо обеспечить мониторинг системы и ее компонентов (включаясетевое оборудование) в режиме 24/7;

2) управление системой должно осуществляться только через автоматизированные средства контроля действий администраторов;

3) необходимо в обязательном порядке настроить и использовать технологию «кластеризации» (минимум - в разных помещениях, предпочтительно на разных

ЦОДах) или входить в состав приложения, обладающего внутренней устойчивостью.

Если кластерные узлы находятся в одном ЦОДе, они должны располагаться в разных

стойках;

4) для данных Систем необходимо использовать подключенные через SAN СХД

верхнего\среднего уровня (не внутренние диски и не DAS);

5) одна копия данных приложения должна располагаться на дисковом массиве на

другой площадке, т.е. настроена СХД реплика;

6) для разных копий данных необходимо использовать разные СХД;

7) необходимы решения PVG striping /Secure Path;

8) необходимо использовать минимум 2 (два) выделенных сетевых адаптера для

передачи данных с внешними сервисами;

9) необходимо выделенное сетевое подключение, используемое для целей РКД для

серверов приложений =>2Tb;

10) необходимо полное, документированное решение по восстановлению после

сбоев (Disaster Recovery);

11) необходимо проводить тестирование восстановления данных согласно

утверждённого и подписанного плана тестирования РКД;

12) необходим действующий контракт(техподдержка) на обслуживание ПО и

аппаратных средств со стороны Вендора ПО\оборудования (время реагирования

24 часа или меньше);

13) не менее одного раза в неделю\день (в зависимости от приложения) следует

производить полное РКД, а также не реже раз в сутки проводить

инкрементальное РКД;

14) РКД следует осуществлять в другой ЦОДе (возможно, расщеплением зеркалав

SAN или через локальную сеть на медиа-сервер);

15) каналы связи между комплектами оборудования должны быть шифрованными.

Для Систем RC3 класса могут применяться один из двух следующих типичных схемх резервирования аппаратного обеспечения:

**Fault Tolerance**

